DETAILED ACTION

1. The Office acknowledges the receipt of Applicant's Request for Continued Examination received March 3, 2010. In response new grounds of rejection have been issued.

Response to Arguments

2. Applicant;s arguments were fully considered but were moot due to new grounds of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 21-25 and 28-31 rejected under 35 U.S.C. 103(a) as being unpatentable over Bruwer et al. (U.S. Patent 5,841,866) in view of Applied Cryptography by Bruce Schneier (hereafter Schneier) and Ostroff (U.S. Patent 7,003,501 B2).

As per claim 21 Bruwer teaches:

A method of activating a chipcard for providing services among a terminal, accessible to a service customer, an infrastructure, comprising a network, and a server connected to the infrastructure and associated with a service provider, the chipcard

having a storage medium containing an activation code and an initial challenge code, wherein the method comprises the steps of:

inserting the chipcard in the terminal, (*see at least Bruwer column 3 line 17 and abstract.* The abstract was cited to make clear that the talk of a "circuit" is a circuit on a card which is a "chipcard") the terminal being connected, via the infrastructure, to the server;

comparing, within the chipcard, an activation challenge code, received from the server and through the infrastructure and the terminal, with the initial challenge code stored in the storage medium; (*see at least Bruwer column 3 lines 18-26.* Presents a challenge authenticating the card.) and

if the activation challenge code equals the initial challenge code, sending the activation code stored in the medium, via the terminal and the infrastructure, to the server for activating a card balance associated with the chipcard. (*see at least Bruwer column 3 lines 30-37.*)

The challenge in Bruwer uses knowledge of an encryption to authenticate the card to the server. The "activation challenge code" is a password another form authentication taught by Schneier. (*See at least Schneier page 52.* Where passwords are given as one form of authentication with a demonstration of the posession of a secret encrpytion key being the next method which is taught in the rest of the cited passage from Sschneier which is applied by Bruwer.) It would have been obvious to a person of ordinary skill in the art to use a password rather than the encryption taught in Bruwer to require less processing ability on the chipcard. Bruwer teaches that the

challenge must be accepted while this may not require that the challenge be verified the verification of a challenge by a smartcard before the smartcard will allow process to proceed is taught by Ostroff. (*See at least Ostroff abstract.* Where it requires that a password be entered correctly before it will provide a proper certificate and will actually provide one that tells that it is receiving improper passwords if it receives to many improper entries.) It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the smartcard respond to a challenge to avoid releasing any secret information. The other difference is that Bruwer has the communication going between the terminal and the card rather than from the card thru the terminal to the server. But under MPEP 2144.04 making something separable is obvious therefore since the difference is the terminal is split into a server and terminal with the terminal interfacing with the card then passing communications to the server and from the server to the card it would have been obvious to a user of ordinary skill in the art at the time the invention was made to split the terminal into a terminal and a server so that the server could maintain a central database to check the validity of requests.

As per claim 22 Bruwer teaches:

The method recited in claim 21 wherein a unique card identifier (ID), in electronic or magnetic form, is present on the chipcard. (*see at least Bruwer column 3 lines 30-44.*)

As per claim 23 Bruwer teaches:

The method recited in claim 22 wherein a result produced by the chipcard, through the comparing step, and stored in the medium shows whether the activation challenge code provided to the chipcard equals the initial challenge code present in the storage medium. (*see at least Bruwer column 3 lines 43-44*)

As per claim 24 Bruwer teaches:

The method recited in claim 23 further comprising the steps of:

receiving by the server, from the terminal and via the infrastructure, the card ID and the result; and

verifying, by the server and through a database accessible by the server, whether the result corresponds to an activation code check associated with the card ID and stored in the database. (*see at least Bruwer column 3 lines 30-44.*)

Bruwer has the communication going between the terminal and the card rather than from the card thru the terminal to the server. But under MPEP 2144.04 making something separable is obvious therefore since the only difference is the terminal is split into a server and terminal with the terminal interfacing with the card then passing communications to the server and from the server to the card it would have been obvious to a user of ordinary skill in the art at the time the invention was made to split the terminal into a terminal and a server so that the server could maintain a central database to check the validity of requests.

As per claim 25 Bruwer teaches:

The method recited in claim 24 wherein the card ID, and the associated activation challenge code, the associated activation code check and a reducible card balance associated with the card ID are located in the database.

As per claim 25 Ex parte Pfeiffer, 135 USPQ 31 (BdPatApp&Int 1961) "As to the rejection of the claims on the prior art references, we do not agree with the appellant that such structural limitations as are not disclosed by the references should be given patentable weight. This argument is applicable to claims drawn to structure and not claims drawn to a method. To be entitled to such weight in method claims, the recited structural limitations therein must affect the method in a manipulative sense and not to amount to the mere claiming of a use of a particular structure, which, in our opinion, is the case here." Teaches that the structure in a method claim is not entitled to patentable weight in this case Bruwer and Schneier teach being able to verify the challenge sent to the card and the challenge received from the card which are the functional parts of the method.

As per claim 28 Bruwer teaches:

The method recited in claim 22 wherein a challenge code present on the chipcard shows status of the chipcard, and the method further comprises the step of setting the challenge code present on the chipcard to the activation challenge code provided by the server to the chipcard. (*see Bruwer column 4 lines 46-52.* The counter status is the chipcard status.)

As per claim 29 Bruwer teaches:

The method recited in claim 28 further comprising the step, performed by the terminal, of reading out the challenge code stored on the chipcard in order to determine the status of the chipcard. (*see Bruwer column 4 lines 46-52.* The counter status is the chipcard status.)

As per claim 30 Bruwer teaches:

The method recited in claim 28 further comprising the step, performed by the server, of setting the challenge code to a predefined value C2 if a reducible card balance associated with the card I D has been exhausted. (*see Bruwer column 4 lines 60-65 and column 6 lines 22-25.* The decrement could not be successfully carried out if the count is down to zero.)

As per claim 31 Bruwer teaches:

The method recited in claim 22 further comprising the step of storing, on the chipcard, the activation challenge code provided by the server to the chipcard. (*see Bruwer column 4 lines 60-65.* Receives the next challenge and stores it.)

5. Claims 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruwer et al. (U.S. Patent 5,841,866) in view of Schneier, Ostroff and Lebouill (U.S. Patent 7,360,078 B1).

As per claim 26 Bruwer teaches:

The method recited in claim 23 further comprising the step, performed by the chipcard, if the server has provided a correct value of the activation challenge code to the chipcard, of assigning the activation code to the result or, (*see Bruwer column 3*

lines 18-26. If the challenge was proper it provides a proper response that allows the transaction to go thru.) if not, of assigning a predefined error code E1 to the result.

While Bruwer does not explicitly teach sending an error code if authentication failed Lebouill taught sending an error code when authentication failed. (*see Lebouill column 10 lines 65–column 11 line 6.*) Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send an error code if the authentication failed.

As per claim 27 Bruwer teaches:

The method recited in claim 26 further
comprising the steps, performed by the terminal, of:
reading out and verifying the result; and
providing a report if the result equals the error code E1.

While Bruwer does not explicitly teach sending an error code if authentication failed Lebouill taught sending an error code and taking further action based on that error code when authentication failed. (*see Lebouill column 12 lines 16-27.* Resetting communications is sending a message to fix the problem which is functionally providing a report for the error code.) Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send an error code if the authentication failed and take further action to try to correct the problem indicated by the error code.

Conclusion

6. Any inquiry concerning this communication from the examiner should be directed to Scott S. Trotter, whose telephone number is 571-272-7366. The examiner can normally be reached on 8:30 AM – 5:00 PM, M-F.

7. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P. Trammell, can be reached on 571-272-6712.

8. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

9. The fax phone number for the organization where this application or proceeding is assigned are as follows:

(571) 273-8300 (Official Communications; including After Final Communications labeled "BOX AF")

(571) 273-6705 (Draft Communications)

sst
June 7, 2010
/KIRSTEN S APPLE/

Primary Examiner, Art Unit 3694